



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,757	11/15/2001	Sami Kilkila	602.357USW1	3174
22865	7590	01/30/2004	EXAMINER	
ALTERA LAW GROUP, LLC 6500 CITY WEST PARKWAY SUITE 100 MINNEAPOLIS, MN 55344-7704			TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	8

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/007,757	KILKKILA, SAMI	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 15 November 2001 .

2a) This action is FINAL.                    2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-17 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-17 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 15 November 2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on \_\_\_\_\_ is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

#### Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some \* c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. 10/007,757 .

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

#### Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6 .

4) Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: \_\_\_\_\_ .

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Rowland (US 6,405, 318)

a. Referring to claim 1:

i. Rowland teaches:

(1) defining in the computer system access right profiles having individual command rights to the operating system of the computer system [i.e., referring to Figure 1, a local controller function 6, that is for “defining in the computer system access right profiles having individual command rights to the operating system of the computer system”. Furthermore, referring to Figure 8, a flow diagram of the control function is shown. The controller 125 receives information about events and receives signature information to identify the user and type of event 126. Because the controller may be local to the system, the system can function in real time for suspicious events (column 7, lines 55-60)], wherein the method further comprises the steps of:

(2) recognizing the need for modification of the access right profiles in the computer system [i.e., referring to Figure 1, a login anomaly detection function 3 and logout anomaly detection function 7, they are for “recognizing the need for modification of the access right profiles in the computer system”. Referring to Figure 3, if the user is not to be ignored and if

the user is logging in to the system, the monitor builds/updates the user profile database 22 and updates the active user database as shown in Figure 4 (column 4, lines 41-44). In addition, turning now to Figures 5A and 5B, flow diagrams of the logout anomaly detection function are shown. When a user attempts to logout, the logout anomaly detector 49 goes through a series of steps to process the logout to determine if something has occurred during the user's login time that may indicate a system anomaly. The logout entry for the user is updated in the user profile and the active user database is updated 50 (column 5, lines 40-47)];

(3) reading the information contained in the access right profiles [i.e., again referring to Figure 3, For each user, a profile is automatically built of the days, times and length of time that the user has logged in. Once a certain threshold number of user logins have occurred for this user to allow for accurate user profiling (usually approximately ten logins, but this can be adjusted by the user), the day and time of the current user's attempted login is compared (that means "reading the information contained in the access right profiles") to that profile. If the current login time differs from the user's login profile, the control function is notified 37 (column 5, lines 22-28)];

(4) establishing which access right profiles have to be modified [i.e., referring to Figure 1, a local controller function 6, that is for "establishing which access right profiles have to be modified". In fact, referring to Figure 8, the controller 125 receives information about events and receives signature information to identify the user and type of event 126. Because the controller may be local to the system, the system can function in real time for suspicious events. In addition, if the controller is local, the intrusion detection system can be located entirely within the local host computer. The controller then determines the action to be taken and takes appropriate action 127. The action may be to log the event to the local system log 128, log the event to a remote system log 129, disable the user's account 130, block access to the attacking host system address 131, trigger a user defined event 132, drop the

route to the offending system 133, block network access from the offending system 134, notify the system administrator 135, to ignore the event 136 or any combination of these actions (column 7, lines 55-67 through column 8, lines 1-3)]; and

(5) modifying the access right profiles dynamically as necessary in view of the need for modification that has been recognized [i.e., the user profile data (signature) is saved and updated every time the user logs on and off the system. The advantage of dynamically building user profile data based on past user behavior and comparing it to that user's current behavior is that the number of false alarms is reduced. In addition, there is no need to enter sets of rules prior to system initialization (column 2, lines 46-52)].

b. Referring to claim 2:

i. Rowland further teaches:

(1) wherein an access right profile comprising one or more user identifiers is defined in the computer system [i.e., there is a need to automatically build profiling data specific for each user or class of users, that is "one or more user identifiers", that can be used to determine normal actions for a user to reduce the occurrence of false alarms and to improve detection (column 2, lines 22-26)].

c. Referring to claim 3:

i. Rowland further teaches:

(1) wherein an access right profile comprising one or more terminals is defined in the computer system [i.e., referring to Figure 9, the central system computer 150 may be part of a network that contains multiple host computer (1 through N) 151-153. Each host 151-153 comprises a local controller that sends information about log auditing, login anomaly detection, logout anomaly detection, session monitoring and port scan detector functions to the central controller (column 8, lines 10-16)].

d. Referring to claim 4:

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified as a function of time [i.e., the odd login time module 184 monitors user logins and attempts to spot "unusual" login times based on past data collected for this user. Odd login times are one of the primary indicators of unauthorized system intrusion. The odd login time module 184 runs only after a predetermined amount of user logins have been collected by the user database. This amount defaults to ten logins, but can be adjusted by the user or system administrator to begin comparing login times after any amount has passed, although sufficient time should be granted to allow accurate profiling (column 1, lines 21-30)].

e. Referring to claim 5:

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified as a function of the utilization rate of the computer system [i.e., the theory of operation to take the average login hours from the login tracking field for a particular user. This average is used to draw conclusions about the user's login habits including the days they log into the computer, the times they log into the computer and how long they stay logged into the computer (column 9, lines 31-36)].

f. Referring to claim 6:

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified when a predetermined alarm situation occurs in the computer system [i.e., The odd login time module 184 runs only after a predetermined amount of user logins have been collected by the user database. This amount defaults to ten logins, but can be adjusted by the user or system administrator to begin comparing login times after any amount has passed, although sufficient time should be granted to allow accurate profiling (column 1, lines 24-30)].

g. Referring to claim 7:

i. Rowland further teaches:

(1) wherein the access right profiles in the computer system are modified as a function of session duration and/or operation commands used and/or number of sessions held [i.e., **the theory of operation to take the average login hours from the login tracking field for a particular user. This average is used to draw conclusions about the user's login habits including the days they log into the computer, the times they log into the computer and how long they stay logged into the computer (column 9, lines 31-36)**].

h. Referring to claim 8:

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

i. Referring to claim 9:

i. Rowland further teaches:

(1) wherein the computer system is a telephone switching system [i.e., referring to Figure 1, "a telephone switching system" is considered to include in the central system controller 150 as shown in Figure 9].

j. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

k. Referring to claim 11:

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

l. Referring to claim 12:

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

m. Referring to claim 13:

i. This claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

n. Referring to claim 14:

i. This claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

Art Unit: 2135

o. Referring to claim 15:

i. This claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

p. Referring to claim 16:

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

q. Referring to claim 17:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

**Conclusion**

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Aucsmith et al (US 5, 940, 513) discloses a method and apparatus for access control in a computer system (see abstract).

b. Abadi et al (US 5, 315, 657) discloses an access control list for determining the access rights of principals in a distributed system to a system resource wherein the access rights of a specified principal are based on the access rights delegated to that principal (see abstract).

c. East et al (US 5, 321, 841) discloses in a multitasking, multiuser computer system, a server process temporarily impersonates the characteristics of a client process when the client process perform a remote procedure call on the server process (see abstract).

d. Langlois et al (US6, 018, 571) discloses An interactive system include a software application and a telephone which function cooperatively to implement a multiplicity of user-invoked features. The telephone set is connected to a computer on which a telephony application program interface application is executed (see abstract).

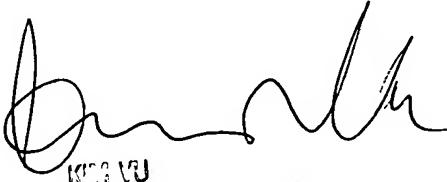
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

January 25, 200404



KIM VU  
CUTTING EDGE PATENT EXAMINER  
TECHNOLOGY CENTER 2100